Department of Homeland Security/National Infrastructure Protection Center CyberNotes

Issue #2003-05 *March 10, 2003*

Effective March 1st the National Infrastructure Protection Center officially moved into the new Department of Homeland Security under the Information Analysis and Infrastructure Protection (IAIP) Directorate.

CyberNotes is published every two weeks by the Department of Homeland Security/National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between February 17 and March 6, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alentum Software, Inc WebLog[1]	Windows	WebLog Expert 1.61, Expert 2.0 Beta 1, Expert Lite 1.61, 2.0 Beta 1	A vulnerability exists because HTML code can be embedded in the HTTP header section of a web log entry, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	WebLog Expert HTTP Header Code Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[1] Bugtraq, March 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alentum Software, Inc.[2]	Windows	WebLog Expert 1.61, 2.0 beta 1	A vulnerability exists due to insufficient sanitization of HTML when logging requests, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	WebLog Expert Logfile Insufficient Sanitization	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
AMX Mod[3]	Multiple	AMX Mod 0.9.2	A format string vulnerability exists in the 'amx_say' command, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AMX Mod Remote 'amx_say' Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Apple[4]	Windows NT 4.0/2000, MacOS X, Unix	Quicktime MP3 Broadcaster	A buffer overflow vulnerability exists due to insufficient bounds checking on MP3 filenames, which could let a remote malicious user execute arbitrary commands.	Update available at: http://docs.info.apple.com/article.html?artnum=70171#English	Apple Quicktime/ Darwin MP3 Broadcaster Filename Buffer Overflow CVE Name: CAN-2003-0055	**High**	Bug discussed in newsgroups and websites.

[2] Bugtraq, March 4, 2003.
[3] void.at Security Advisory VSA0308, February 26, 2003.
[4] @stake, Inc. Security Advisory, February 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[5]	Windows NT 4.0/2000, MacOS X, Unix	Darwin Streaming Server 4.1.2, Quicktime Streaming Server 4.1.1	Multiple vulnerabilities exist: a vulnerability exists in the 'parse_xml.cgi' application due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code; a path disclosure vulnerability exists in the 'parse_xml.cgi' application which could let a remote malicious user obtain sensitive information; a directory listing vulnerability exists in the 'parse_xml.cgi' application when the open() function is used to open the inode of a directory as a file, which could let a remote malicious user obtain sensitive information; a Cross-Site Scripting vulnerability exists due to the way the 'parse_xml.cgi' generates error messages when a filename which does not exist is passed as the 'filename' parameter, which could let a remote malicious user execute arbitrary code; a vulnerability exists when viewing QTSS logs, which could let a remote malicious user execute arbitrary code; a vulnerability exists due to insufficient sanitization of some parameters given to the 'parse_xml.cgi' script, which could let a malicious user obtain sensitive information; and a vulnerability exists because information is revealed when certain requests are made, which could let a malicious user obtain sensitive information.	Update available at: http://docs.info.apple.com/article.html?artnum=70171#English	Apple QuickTime/ Darwin Multiple Vulnerabilities CVE Names: CAN-2003-0050, CAN-2003-0051, CAN-2003-0052, CAN-2003-0053, CAN-2003-0054	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for some of these vulnerabilities.

[5] @stake, Inc. Security Advisory, February 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Archimede[6]	Unix	Glftpd 1.25-1.28	Multiple vulnerabilities exist: a vulnerability exists because the messaging system allows authenticated users to append a formatted line to any file on the system, which could let a remote malicious user obtain root access; a vulnerability exists in the 'unzip' function because a specially crafted command argument may be submitted, which could let a remote malicious user obtain sensitive information; and a vulnerability exists in certain configuration files, which could let a remote malicious user obtain root access.	No workaround or patch available at time of publishing.	Glftpd Multiple Vulnerabilities	Medium/ **High** **(High if root access can be obtained)**	Bug discussed in newsgroups and websites. There is no exploit code required.
aterm[7]	Unix	aterm 0.42	A vulnerability exists in the MenuBar feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	ATerm Menu Bar Escape Sequence Command Execution CVE Name: CAN-2003-0024	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Axis Communications[8]	Multiple	2100 Network Camera 2.00- 2.03, 2.12, 2.30-2.33, 2130 PTZ Network Camera 2.32, 2400 Video Server 1.01, 1.02, 1.10-1.12, 1.15, 2.20, 2.31-2.33	Several vulnerabilities exist: a vulnerability exists because sensitive information is not properly secured, which could let a malicious user obtain sensitive information; and a vulnerability exists in the ‘command.cgi’ script because input is not properly handled, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	No workaround or patch available at time of publishing.	Axis Communications Multiple Vulnerabilities	Low/ Medium/ **High** **(Low if a Denial of Service; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
BYTE/ 400[9]	Windows	Platinum FTPserver 1.0.10, 1.0.11	A Directory Traversal vulnerability exists which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PlatinumFTP Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited with an FTP client.

[6] Bugtraq, February 23, 2003.
[7] Bugtraq, February 24, 2003.
[8] 2002@WebSec.org Security Report, February 28, 2003.
[9] SecurityTracker Alert, 1006159, February 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[10]	Multiple	IOS 11.1-12.0	A buffer overflow vulnerability exists when a malformed OSPF (Open Shortest Path First) packet is submitted, which could let a malicious user cause a Denial of Service or execute arbitrary code.	Cisco customers should contact the vendor for details on obtaining fixes.	Cisco IOS OSPF Neighbor Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Coffee Cup Software[11]	Multiple	Password Wizard 4.0	A vulnerability exists in the default configuration because usernames and passwords are insufficiently protected, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CoffeeCup Software Password Wizard Remote Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
CutePHP Team[12]	Windows, Unix	CuteNews 0.88	A vulnerability exists in the 'shownews.php', 'search.php', and 'comments.php' scripts because files can be included without validating the location of the included file, which could let a remote malicious user execute arbitrary system commands.	No workaround or patch available at time of publishing.	CuteNews Remote File Include	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Ecartis Project [13]	Unix	Ecartis 1.0.0 snapshot 20021013	An authentication vulnerability exists in the e-mail list management software, which could let a remote malicious user modify authentication information.	Upgrade available at: www.ecartis.org	Ecartis Password Modification	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ehud Gavron[14] ***Debian issues upgrade***[15]	**Unix**	**TrACES route 6.0, 6.1, 6.1.1**	**A format string vulnerability exists in the terminator (-T) function due to improper use of the fprint function, which could let a malicious user obtain root privileges.**	***Debian:*** **http://security.debian.org/pool/updates/main/t/traceroute-nanog/**	**TrACESroute Terminator Function Format String** **CVE Name: CAN-2002-1051**	**High**	**Bug discussed in newsgroups and websites.**
Ehud Gavron[16] ***Debian issues upgrade***[17]	**Unix**	**TrACES route 6.0, 6.1, 6.1.1**	**Two buffer overflow vulnerabilities exist due to insufficient bounds checking, which could let a malicious user execute arbitrary code.**	**Upgrade available at:** **ftp://ftp.suse.com/pub/suse/** ***Debian:*** **http://security.debian.org/pool/updates/main/t/traceroute-nanog/**	**Traceroute-Nanog Buffer Overflow Vulnera-bilities** **CVE Names: CAN-2002-1386, CAN-2002-1387**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[10] SecurityFocus, February 21, 2003.
[11] Bugtraq, February 28, 2003.
[12] SecurityFocus, February 25, 2003.
[13] Bugtraq, March 3, 2003.
[14] DownBload Security Research Lab Advisory, June 6, 2002.
[15] Debian Security Advisory, DSA 254-1, February 27, 2003.
[16] SuSE Security Announcement, SuSE-SA:2002:043, November 12, 2002.
[17] Debian Security Advisory, DSA 254-1, February 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Electronic Arts Inc.[18]	Multiple	Battlefield 1942 1.2, 1942 1.3	A vulnerability exists due to insufficient checking of user-supplied input to the administration port of a game server, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	Battlefield 1942 Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
file[19, 20, 21]	Unix	file 3.28, 3.30, 3.32-3.37, 3.39, 3.40	A buffer overflow vulnerability exists in the file utility ELF parsing routines, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.	Upgrade available at: ftp://ftp.gw.com/mirrors/ pub/unix/file/file-3.41.tar.gz **RedHat:** ftp://updates.redhat.com/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/	File ELF Routine Buffer Overflow CVE Name: CAN-2003-0102	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
FreeBSD[22]	Unix	FreeBSD 4.5-4.7, 5.0	A vulnerability exits in the implementation of syncookies because generated keys are 32 bits in length, which could let a malicious user bypass IP based access control lists.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:03/syncookie.patch	FreeBSD syncookies TCP Initial Sequence Number Weakness	Medium	Bug discussed in newsgroups and websites.
Frisk Software[23]	Unix	F-Prot Antivirus for Linux & BSD 3.12 b	A buffer overflow vulnerability exists in file name parameters that are passed to the command line scanner, which could let a malicious user execute arbitrary code.	Upgrade available at: http://subscription.f-prot.com/download.html	F-Prot Antivirus Command Line Scanner Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
GNOME[24, 25, 26]	Unix	gnome-terminal 2.1-2.2.1	A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.	**RedHat:** ftp://updates.redhat.com/8.0/en/os/	Gnome-Terminal Window Title Reporting Escape Sequence Command CVE Name: CAN-2003-0070	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[18] void.at Security Advisory VSA0307, February 26, 2003.
[19] OpenPKG Security Advisory, OpenPKG-SA-2003.017, March 4, 2 003.
[20] Mandrake Linux Security Update Advisory, MDKSA-2003:030, March 6, 2003.
[21] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:086-07, March 7, 2003.
[22] FreeBSD Security Advisory, FreeBSD-SA-03:03, February 24, 2003.
[23] SecurityFocus, February 26, 2003.
[24] Bugtraq, February 24, 2003.
[25] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:053-10, February 24, 2003.
[26] Gentoo Linux Security Announcement, 200303-2, March 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
GONi-CUS [27]	Unix	System Administrator 1.0	A vulnerability exists in several PHP pages that are in the /plugins and /includes folders, which could let a remote malicious user execute arbitrary system commands.	No workaround or patch available at time of publishing.	System Administrator Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
GT Catalog[28]	Windows, Unix	GTCatalog 0.8.16, 0.9, 0.9.1	A vulnerability exists in the 'index.php' file due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	GTCatalog Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Gzip.org [29]	Unix	zlib 1.1.4	A buffer overflow vulnerability exists in the compression library due to insufficient bounds checking of user-supplied data to the gzprintf() function, which could let a malicious user execute arbitrary instructions.	**OpenPKG:** http://www.openpkg.org/security/OpenPKG-SA-2003.015-zlib.html	Zlib gzprintf() Buffer Overflow CVE Name: CAN-2003-0107	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Hanterm[30]	Unix	hanterm-xf 2.0	A Denial of Service vulnerability exists because the terminal fails to sufficiently filter certain potentially malicious loop-based escape sequences.	No workaround or patch available at time of publishing.	Hanterm-XF Loop-Based Escape Sequence Denial of Service CVE Name: CAN-2003-0079	Low	Bug discussed in newsgroups and websites.
Hanterm[31]	Unix	hanterm-xf 2.0	A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	hanterm-xf Window Title Reporting Escape Sequence Command CVE Name: CAN-2003-0078	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Company [32]	Unix	Tru64 5.1 PK6 (BL20)	A vulnerability exists in the XFS implementation, which could let a malicious user cause a Denial of Service and obtain elevated privileges.	Patch available at: http://ftp.support.compaq.com/patches/public/unix/v5.1/t64v51b20-c0165900-17027-es-20030220.tar	Tru64 Unspecified XFS	Low/ Medium (Medium if elevated privileges can be obtained)	Bug discussed in newsgroups and websites.

[27] SecurityFocus, February 24, 2003.
[28] Bugtraq, March 3, 2003.
[29] OpenPKG Security Advisory, OpenPKG-SA-2003.015, March 4, 2003.
[30] Bugtraq, February 24, 2003.
[31] Bugtraq, February 24, 2003.
[32] Hewlett Packard Company Security Bulletin, SSRT2422, March 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company[33]	Multiple	JetDirect J3263A, J3113A, J3111A, J3110A, J2591A, J2552B, J2552A, 300.0 X	A vulnerability exists in the SNMP support function because the password can be retrieved, which could let a remote malicious user access and change configuration of the printer.	No workaround or patch available at time of publishing.	JetDirect Printer Password Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hyper mail[34] ***Debian issues upgrade[35]*** ***SuSE issues upgrade[36]***	**Unix**	**Hypermail 2.1.3, 2.1.4, 2.1.5**	**Several buffer overflow vulnerabilities exist: a buffer overflow vulnerability exists in the parsemail() function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'mail' CGI component when a reverse DNS lookup is performed if the hostname is of excessive length, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the mail CGI program, which could let a remote malicious user send e-mail to arbitrary recipients.**	**Upgrade available at: http://sourceforge.net/project/showfiles.php?group_id=18117&release_id=135937** ***Debian:*** **http://security.debian.org/pool/updates/main/h/hypermail/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse/**	**Hypermail Remote Buffer Overflows** **CVE Name: CAN-2003-0057**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**
Hyper-Mail[37]	Unix	HyperMail 2.0 b25, 2.1.0, 2.1.2-2.1.4	A vulnerability exists which could let a remote malicious user abuse the service as an open mail relay.	SuSE: ftp://ftp.suse.com/pub/suse/i386/update/	Hypermail CGI Mail Open Relay CVE Name: CAN-2003-0025	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hyper-Mail[38]	Unix	HyperMail 2.0 b25, 2.1.0, 2.1.2-2.1.4	A race condition vulnerability exists because files are created in temporary directories, which could let a malicious user overwrite files.	SuSE: ftp://ftp.suse.com/pub/suse/	Hypermail Local Temporary File Race Condition	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[33] Bugtraq, March 6, 2003.
[34] Bugtraq, January 27, 2003.
[35] Debian Security Advisory, DSA 248-1, January 31, 2003.
[36] SuSE Security Announcement, SuSE-SA:2003:0012, February 27, 2003.
[37] SuSE Security Announcement, SA:2003:0012, February 27, 2003.
[38] SuSE Security Announcement, SuSE-SA:2003:0012, February 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[39]	Multiple	4758, CMOS Cryptographic Coprocessor, Common Cryptographic Architecture 2.40, 2.41	Vulnerabilities exist in the APIs used by various ATM Hardware Security Modules (HSM) to protect customer PIN numbers, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple Vendor ATM Hardware Security Module PIN Generation/ Verification	Medium	Bug discussed in newsgroups and websites.
IBM Lotus[40]	Windows NT 4.0/2000, Unix	Lotus Domino 6.0	A Denial of Service vulnerability exists when a malicious user submits specially malformed HTTP POST requests.	Upgrade available at: http://www14.software.ibm.com/webapp/download/search.jsp?q=&cat=&pf=&k=&dt=&go=y&rs=ESD-DMNTSRVRi&S_TACT=&S_CMP=&sb=r	Lotus Domino Web Server HTTP POST Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Indigo STAR Software[41]	Unix	Perl2Exe 1.0 9, 5.0 2, 6.0	A vulnerability exists when the 'encrypt' option is selected because Perl programs compiled into EXEs with Perl2Exe can be decompiled and full source code extracted, which could result in a false sense of security.	The vendor has acknowledged this issue and stated that Perl2Exe should be not be used to obfuscate Perl source code.	Perl2Exe Code False Sense of Security	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Instant Servers, Inc.[42]	Windows NT 4.0/2000, XP	ISMail 1.4.3	A buffer overflow vulnerability exists in the SMTP service because long strings are not properly handled, which could let a remote malicious user execute arbitrary code.	Patch available at: http://instantservers.com/download/ism145.exe	ISMail Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Institute for Open Systems Technology Australia Peter Werner[43]	Unix	login_ldap 3.1, 3.2	A vulnerability exists in the 'login_ldap' module when used in conjunction with specific LDAP server configurations, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: http://www.ifost.org.au/~peterw/login_ldap-3.3.tar.gz	login_ldap Module Unauthorized Access	Medium	Bug discussed in newsgroups and websites.
Invision Power Services[44]	Unix	Invision Board 1.1.1	A vulnerability exists in the 'ipchat.php' script due to insufficient sanitization or user-supplied data in URI parameters, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Invision Board Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[39] Bugtraq, February 20, 2003.
[40] NGSSoftware Insight Security Research Advisory, NISR17022003d, February 17, 2003.
[41] Bugtraq, February 21, 2003.
[42] NGSSoftware Insight Security Research Advisory, February 27, 2003.
[43] Bugtraq, February 21, 2003.
[44] Bugtraq, February 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iPlanet[45]	Windows NT 4.0/2000, Unix	Web Server 6.0	A vulnerability exists because a log entry may be concealed using a hostname that is prepended with a malicious string, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	iPlanet Web Server Concealed Log Entry	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
iPlanet E-Com-merce Solutions[46]	Windows NT 4.0/2000, Unix	Web Server 4.1, 4.1 SP1- SP12, 6.0, 6.0 SP1&2, Enterprise Edition 4.0, 4.0 SP1-SP6, 4.1, 4.1 SP1-SP11, 6.0, 6.0 SP1&2,	A vulnerability exists due to insufficient sanitization of HTML when logging requests, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	iPlanet Log Analyzer Logfile HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[45] Bugtraq, March 4, 2003.

[46] Bugtraq, March 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ISC[47, 48, 49, 50, 51, 52, 53] ***Hewlett Packard issued patch***[54]	**Unix**	**FreeBSD FreeBSD 4.4-4.7; ISC BIND 8.1-8.1.2, 8.2-8.2.6, 8.3.0-8.3.3; OpenBSD OpenBSD 3.0-3.2**	**Multiple vulnerabilities exist: a buffer overflow vulnerability exists in 'named' when responses are constructed using previously-cached malformed SIG records, which could let a remote malicious user execute arbitrary code; a Denial of Service vulnerability exists due to a failure to properly handle DNS lookups for non-existent sub-domains when overly large OPT resource records are appended to a query; and remote Denial of Service vulnerability exists due to a failure to properly dereference cache SIG RR elements that contain invalid expiry times from the internal database.**	**FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:43/bind.patch** **SuSE:** **ftp://ftp.suse.com/pub/suse/** **Debian:** **http://security.debian.org/pool/updates/main/b/bind/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **EnGarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **ISC:** **http://www.isc.org/products/BIND/patches/bind826.diff** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/** ***Hewlett Packard:*** **http://ftp.support.compaq.com/patches/public/unix/v4.0f/duv40fb18-c0090600-16637-es-20030129.README**	**BIND Multiple Vulnerabilities** **CVE Names: CAN-2002-1219, CAN-2002-1220, CAN-2002-1221**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
LBL[55] ***More patches releases***[56, 57]	**Unix**	**tcpdump 3.4 a6, 3.4, 3.5, 3.5.2, 3.6.2**	**A vulnerability exists due to a miscalculation in the use of the sizeof operator, which could let a malicious user cause a Denial of Service or execution of arbitrary code.**	**SCO:** **ftp://ftp.sco.com/pub/updates/OpenLinux/** **Trustix:** http://www.trustix.net/pub/Trustix/updates/ ***Debian:*** **http://security.debian.org/pool/updates/main/t/tcpdump/** *Mandrake:* **http://www.mandrakesecure.net/en/ftp.php**	**TCPDump Memory Corruption**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**

[47] CERT® Advisory CA-2002-31, November 14, 2002.
[48] Conectiva Linux Security Announcement, CLA-2002:546, November 14, 2002.
[49] Debian Security Advisory, DSA 196-1, November 14, 2002.
[50] EnGarde Secure Linux Security Advisory, ESA-20021114-029, November 14, 2002.
[51] FreeBSD Security Advisory, FreeBSD-SA-02:43, November 14, 2002.
[52] Mandrake Linux Security Update Advisory, MDKSA-2002:077, November 14, 2002.
[53] SuSE Security Announcement, SuSE-SA:2002:044, November 14, 2002.
[54] Hewlett Packard Company Security Bulletin, HPSBUX0212-233, February 20, 2003.
[55] SCO Security Advisory, CSSA-2002-050.0, November 20, 2002.
[56] Debian Security Advisory, DSA 255-1, February 27, 2003.
[57] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
LBL[58, 59, 60, 61, 62]	Unix	tcpdump 3.5.2, 3.6.2, 3.7, 3.7.1	A remote Denial of Service vulnerability exists when maliciously formatted ISAKMP packets are submitted.	Upgrade available at: http://www.tcpdump.org/release/tcpdump-3.7.2.tar.gz **Debian:** http://security.debian.org/pool/updates/main/t/tcpdump/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.2/UPD/tcpdump-3.7.1-1.2.1.src.rpm **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	TCPDump Malformed ISAKMP Packet Remote Denial of Service CVE Name: CAN-2003-0108	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
LBL[63, 64, 65, 66, 67, 68] ***More patches released***[69, 70]	**Unix**	**tcpdump 3.6.2**	**A remote buffer overflow vulnerability exists when malformed NFS packets are handled, which may let a remote malicious user execute arbitrary instructions with the privileges of the tcpdump process.**	**Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **RedHat:** **ftp://updates.redhat.com/** **Caldera:** **ftp://ftp.caldera.com/pub/updates/OpenLinux/** **SuSE:** **ftp://ftp.suse.com/pub/suse/** **Mandrake Linux:** **http://www.mandrakesecure.net/en/ftp.php** **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:29/tcpdump.patch **Trustix:** http://www.trustix.net/pub/Trustix/updates/ *Debian:* **http://security.debian.org/pool/updates/main/t/tcpdump/** *Mandrake:* **http://www.mandrakesecure.net/en/ftp.php**	**TCPDump Malformed NFS Packet Buffer Overflow** **CVE Name: CAN-2002-0380**	**High**	**Bug discussed in newsgroups and websites.**

[58] iDEFENSE Security Advisory, February 27, 2003.
[59] Debian Security Advisory, DSA 255-1, February 27, 2003.
[60] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.
[61] OpenPKG Security Advisory, OpenPKG-SA-2003.014, March 4, 2003.
[62] Gentoo Linux Security Announcement, 200303-5, March 5, 2003.
[63] Conectiva Linux Security Announcement, CLA-2002:491, June 6, 2002.
[64] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:094-08, May 29, 2002.
[65] Caldera International, Inc. Security Advisory, CSSA-2002-025.0, June 4, 2002.
[66] SuSE Security Announcement, SuSE-SA:2002:020, May 29, 2002.
[67] Mandrake Linux Security Update Advisory, MDKSA-2002:032, May 16, 2002.
[68] Hewlett-Packard Company Security Advisory, HPSBTL0205-044, June 1, 2002.
[69] Debian Security Advisory, DSA 255-1, February 27, 2003.
[70] Mandrake Linux Security Update Advisory, MDKSA-2003:027, March 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Light httpd[71] ***More exploit scripts published***[72]	**Windows, Unix**	**Light HTTPD 0.1**	**A buffer overflow vulnerability exists when an overly long GET request is submitted, which could let a remote malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Light HTTPD Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit scripts have been published.***
Macromedia[73]	Windows	Flash 6.0, 6.0.29.0, 6.0.40.0, 6.0.47.0, 6.0.65.0	Two buffer overflow vulnerabilities exists that affects (read/write) and sandbox integrity, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.macromedia.com/go/getflashplayer/	Macromedia Flash Player Remote Buffer Overflows	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Mambo server. com[74]	Windows, Unix	Mambo Site Server 4.0.12 RC2	A vulnerability exists in the '/administrator/index2.php' script due to insufficient credential authentication, which could let a remote malicious user obtain administrative access.	Upgrade available at: http://prdownloads.sourceforge.net/mambo/MamboV4.0.12-RC3.tar.gz?download Patch available at: http://prdownloads.sourceforge.net/mambo/MamboV4.0.12-RC3-patch.tar.gz?download	Mambo Site Credential Authentication	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Matt Wright[75]	Unix	WWW Board 2.0 Alpha 2.1, 2.0 Alpha 2	A Cross-Site Scripting vulnerability exists in the message posting page due to insufficient sanitization of user-supplied forum input, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	WWWBoard Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
mhc-utils[76]	Unix	mhc-utils 0.25 - snap20010625	A vulnerability exists in the 'adb2mhc' utility because temporary files are created in an insecure manner, which could let a malicious user corrupt or modify another user's data.	**Debian:** http://security.debian.org/pool/updates/main/m/mhc/	mhc-utils Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Michael Wihsbock[77]	Windows, Unix	WihPhoto 0.86 -dev	An input validation vulnerability exists in the 'sendphoto.php' script due to insufficient URI parameter verification, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WihPhoto Input Validation	Medium	Bug discussed in newsgroups and websites. Proof of Concepts exploits have been published.

[71] INetCop Security Advisory, 2002-0x82-002, November 12, 2002.
[72] SecurityFocus, March 4, 2003.
[73] Macromedia Security Bulletin, MPSB03-03, March 5, 2003.
[74] Bugtraq, February 24, 2003.
[75] Security Corporation Security Advisory, SCSA-007, February 23, 2003.
[76] Debian Security Advisory, DSA 256-1, February 28, 2003.
[77] Bugtraq, February 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Michael Jennings[78]	Unix	Eterm 0.8.10, 0.9.1	A vulnerability exists because the screen dump feature may be abused to corrupt local files that are writeable by the terminal user, which could let a local/remote malicious user obtain elevated privileges.	Upgrade available at: http://www.eterm.org/download/	Eterm Screen Dump Escape Sequence CVE Name: CAN-2003-0021	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[79]	Windows ME, XP	Windows ME, XP Home, XP Professional	A buffer overflow vulnerability exists in the URL Handler for Help and Support Center due to insufficient bounds checking of user-supplied input, which could let a malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-006.asp	Windows Help & Support Center Buffer Overflow CVE Name: CAN-2003-0009	**High**	Bug discussed in newsgroups and websites.
Microsoft[80]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.0, 5.5, 5.5 SP1&2, 6.0, 6.0 SP1	A vulnerability exists because script code that is within an HTML document is allowed to run as an embedded executable file, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	Internet Explorer Self Executing HTML File	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft[81]	Windows 95/98/ME/ NT 4.0/2000	Outlook 2000, 2000 SR1, 2000 SP2, Outlook Express 6.0	A vulnerability exists when an e-mail or newsgroup message is viewed using Outlook because a temporary object is created in the Internet Explorer cache and the security zone is set to the Internet Zone by default, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft Outlook and Outlook Express Arbitrary Program Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[78] Bugtraq, February 24, 2003.
[79] Microsoft Security Bulletin, MS03-006, February 26, 2003.
[80] Bugtraq, February 25, 2003.
[81] NTBugtraq, February 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [82] *Microsoft updates bulletin*[83]	Windows 98/ME/NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, 98, 98 a/b/j, 98SE, ME, NT Server 4.0, NT Server 4.0 SP1-SP6a, NT Terminal Server 4.0, alpha, SP1-SP6a, NT Workstation 4.0, 4.0 SP1-SP6a, Windows XP, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	Two vulnerabilities exist: a buffer overflow vulnerability exists in a function that is exposed in an ActiveX control, which could let a malicious user execute arbitrary code; and a vulnerability exists due to flaws associated with the handling of compiled HTML Help (.chm) files that contain shortcuts, which could let a malicious user execute arbitrary commands. *Microsoft updated bulletin to reflect an updated Windows XP patch.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-055.asp	Microsoft Windows Help Facilities CVE Names: CAN-2002-0693, CAN-2002-0694	High	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.

[82] Microsoft Security Bulletin, MS02-055, October 2, 2002.
[83] Microsoft Security Bulletin, MS02-055 V1.1, February 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[84] *Exploit script published*[85]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, Japanese Edition, Terminal Services, SP1-SP3, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability in the Locator service due to inadequate parameter checks, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms03-001.asp	Windows Locator Service Buffer Overflow CVE Name: CAN-2003-0003	Low/High (High if arbitrary code is executed)	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media. *Proof of Concept exploit script has been published.*
MIT[86] *Patch now available*[87]	Unix	PGP Public Key Server 0.9.2, 0.9.4	A buffer overflow vulnerability exists because long search strings are not handled properly which could let a remote malicious user overwrite stack variables, including the return address.	*Patch available at:* http://www.rubin.ch/pgp/src/patch_buffoverflow20020525	PGP Public Key Server Remote Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published

[84] Microsoft Security Bulletin, MS03-001, January 22, 2003.
[85] SecurityFocus, February 27, 2003.
[86] Bugtraq, May 24, 2002.
[87] SecurityFocus, February 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[88] ***Mandrake issues upgrade***[89]	**Unix**	**RedHat Linux 7.2, 7.2 ia64, 7.3, 8.0**	**A vulnerability exists in the 'useradd' utility due to a failure to set secure permissions for a new user's mail spool directory, which could let a malicious user obtain sensitive information.**	**Upgrade available at:** **ftp://updates.redhat.com/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	***Multiple Vendor*** **useradd Insecure Mail Spool Permissions** **CVE Name: CAN-2002-1509**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

Multiple Vendors[90]	Unix	HP HP-UX 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22;
		IBM AIX 4.3-4.3.3, 5.1, 5.2;
		SGI IRIX 5.0, 5.0.1, 5.1, 5.1.1, 5.2, 5.3, 6.0, 6.0.1, 6.1-6.5.19, 6.5.2 m-6.5.18 m, 6.5.2 f-6.5.18 f;
		Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86
			A vulnerability exists in dtterm's window title reporting feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	DTTerm Window Title Reporting Escape Sequence Command
					CVE Name: CAN-2003-0064
						High	Bug discussed in newsgroups and websites. There is no exploit code required.

Multiple Vendors[91]	Multiple	Galeon Galeon Browser 1.2.6;
		Mozilla Browser 1.0.1, 1.1;
		Netscape Navigator 6.0, 7.0
			A Denial of Service vulnerability exists in Netscape based browsers when interpreting certain style sheet code.	No workaround or patch available at time of publishing.	Netscape Style Sheet Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[88] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:057-06, February 18, 2003.
[89] Mandrake Linux Security Update Advisory, MDKSA-2003:026, February 27, 2003.
[90] Bugtraq, February 24, 2003.
[91] Bugtraq, February 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[92, 93, 94, 95]	Unix	EnGarde Guardian Digital WebTool 1.2; Webmin Usermin 0.4- 0.99, 1.0 50, 1.0 60	A vulnerability exists in the 'Miniserv.pl' script due to insufficient sanitization of client-supplied BASE64 encoded input, which could let a malicious user bypass authentication procedures and obtain administrative access.	**EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/noarch/ **Webmin:** http://www.webmin.com/udownload.html **Mandrake:** http://www.mandrakesecure.net/en/ftp.php	Webmin/ Usermin 'Miniserv.pl' Authentication Bypass CVE Name: CAN-2003-0101	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors [96, 97] ***SGI re-releases bulletin***[98] ***Sun releases patches***[99]	**Mac OS X 10.X, Unix**	**Apple MacOS X 10.0-10.0.4, 10.1-10.1.5, 10.2 (Jaguar), 10.2.1, MacOS X Server 10.0, 10.2-10.2.1; GNU glibc 2.0-2.0.6, 2.1, 2.1.1-6, 2.1.1-2.1.3, 2.1.3-10, 2.2-2.2.5, 2.3, 2.3.1; SGI IRIX 6.5-6.5.13, 6.5.14 m-6.5.17 m, 6.5.14 f-6.5.14 m** ***SGI IRIX 6.5-6.5.13, 6.5.14 m-6.5.17 m, 6.5.14 f-6.5.14 m***	**A remote Denial of Service vulnerability exists in multiple libc implementations that are based on Sun RPC due to a failure to provide a time-out mechanism when reading data from TCP connections.** ***The patches referenced in the original bulletin are incompatible with each other, so SGI has created a new series of patches that address these vulnerabilities and are compatible with each other..***	**SGI:** **ftp://patches.sgi.com/support/free/security/patches/** ***Sun Microsystems:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F51082**	**Multiple Vendor Sun RPC LibC Remote Denial of Service** **CVE Name: CAN-2002-1265**	**Low**	**Bug discussed in newsgroups and websites.**

[92] Gentoo Linux Security Announcement, 200302-12, February 22, 2003.
[93] Gentoo Linux Security Announcement, 200302-14, February 24, 2003.
[94] EnGarde Secure Linux Security Advisory, ESA-20030225-006, February 25, 2003.
[95] Mandrake Linux Security Update Advisory, MDKSA-2003:025, February 26, 2003.
[96] CERT/CC Vulnerability Note VU#266817, November 4, 2002.
[97] SGI Security Advisory, 20021103-01-P, November 8, 2002.
[98] SGI Security Advisory, 20021103-02-P, January 22, 2003.
[99] Sun Alert ID, 51082, February 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [100, 101]	Multiple	Cisco IP Phone Model 7940/7960 running SIP images prior to 4.2, IOS 12.2T and 12.2 'X' trains, PIX Firewall 5.2(1) and up to, but not including versions 6.2(2), 6.1(4), 6.0(4) & 5.2(9); IPTel SIP Express Router 0.8.8, 0.8.9; Nortel Networks Succession Communication Server 2000, 2000 - Compact	Numerous vulnerabilities exist due to the way Session Initiation Protocol (SIP) INVITE messages are handled, which could let a malicious user obtain unauthorized privileged access or cause a Denial of Service. *Note: Specific impacts will vary from product to product.*	**IPTel:** http://www.iptel.org/ser/security/ **Cisco:** www.cisco.com/warp/public/707/cisco-sa-20030221-protos.shtml	Multiple Vendor Session Initiation Protocol Vulnerabilities	Low/ Medium (Medium if privileged access is obtained)	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

[100] CER® Advisory, CA-2003-06, February 21, 2003.
[101] Cisco Security Advisory, February 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors [102, 103, 104, 105, 106, 107, 108, 109, 110, 111]	Unix	FreeBSD 4.2-4.6, 4.6.2, 4.7, 4.7 Stable, 4.8 –PRE-RELEASE, 5.0;
		OpenBSD OpenBSD 3.1, 3.2;
		OpenSSL Project OpenSSL 0.9.1 c, 0.9.2 b, 0.9.3, 0.9.4, 0.9.5 a, 0.9.5, 0.9.6, 0.9.6 a-0.9.6 e, 0.9.6 g, 0.9.6 h, 0.9.7, 0.9.7 beta1-beta3
			A vulnerability exists in implementations of SSL when CBC encryption is used because MAC computation is not performed if an incorrect block cipher padding is used, which could let a remote malicious user obtain sensitive information through analysis of the timing of certain operations.	**FreeBSD:**
				ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:02/
				OpenBSD:
				ftp://ftp.openbsd.org/pub/OpenBSD/patches/
				OpenSSL Project:
				http://www.openssl.org/source/openssl-0.9.6i.tar.gz
				SuSE:
				ftp.suse.com/pub/suse/i386/update/
				OpenPKG:
				ftp://ftp.openpkg.org/release
				Debian:
				http://security.debian.org/pool/updates/main/o/openssl/
				Conectiva:
				ftp://atualizacoes.conectiva.com.br/
				EnGarde:
				ftp://ftp.engardelinux.org/pub/engarde/stable/updates/
				Trustix:
				ftp://ftp.trustix.net/pub/Trustix/updates/
					OpenSSL CBC Error Information Leakage
					CVE Name: CAN-2003-0078
						Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[102] OpenPKG Security Advisory, OpenPKG-SA-2003.013, February 19, 2003.
[103] OpenSSL Security Advisory, February 19, 2003.
[104] Gentoo Linux Security Announcement, 200302-10, February 20, 2003.
[105] EnGarde Secure Linux Security Advisory, ESA-20030220-005, February 20, 2003.
[106] Mandrake Linux Security Update Advisory, MDKSA-2003:020, February 21, 2003.
[107] Trustix Secure Linux Security Advisory, TSLSA-2003-0005, February 21, 2003.
[108] Conectiva Linux Security Announcement, CLA-2003:570, February 24, 2003.
[109] Debian Security Advisory, DSA 253-1, February 24, 2003.
[110] FreeBSD Security Advisory, FreeBSD-SA-03:02, February 25, 2003.
[111] SuSE Security Announcement, SuSE-SA:2003:011, February 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [112]	Unix	SendMail Pro (all versions), SendMail Switch 2.1 prior to 2.1.5, Switch 2.2 prior to 2.2.5, Switch 3.0 prior to 3.0.3, SendMail for NT 2.X prior to 2.6.2, 3.0 prior to 3.0.3, Systems running open-source SendMail versions prior to 8.12.8, including UNIX and Linux systems	A buffer overflow vulnerability exists in the SMTP header parsing component, which could let a malicious user execute arbitrary code using super-user (root) access/control. *Note: Remote malicious users may gain access to other systems through a compromised SendMail server, depending on local configurations.*	**Check with your vendor for an update/patch.** **SendMail:** ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.security.cr.patch ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.11.6.security.cr.patch ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.9.3.security.cr.patch **Apple:** http://docs.info.apple.com/article.html?artnum=61798 **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/s/sendmail/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:04/ **HP:** http://itrc.hp.com **IBM:** ftp://ftp.software.ibm.com/aix/efixes/security/sendmail_efix.tar.Z **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.2/UPD/ **RedHat:** ftp://updates.redhat.com/ **SendMail, Inc.** http://www.sendmail.com/support/download/ **SGI:** ftp://patches.sgi.com/support/free/security/advisories/20030301-01-P **Sun Cobalt:** ftp://ftp-eng.cobalt.com/pub/experimental/security/sendmail/ **Sun Solaris:** http://sunsolve.sun.com/pub-cgi/ **SuSE:** ftp://ftp.suse.com/pub/suse/	SendMail Header Processing Buffer Overflow CVE Name: CAN-2002-1337	**High**	Bug discussed in newsgroups and websites. Exploit script has been published. A Trojan has been published that exploits this vulnerability. Vulnerability has appeared in the press and other public media.

[112] DHS/NIPC Advisory 03-004, March 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
National University of Singapore[113]	Unix	uxterm 2.3, 2.4.1	A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	UXTerm Window Title Reporting Escape Sequence Command CVE Name: CAN-2003-0065	High	Bug discussed in newsgroups and websites. There is no exploit code required.
nCipher[114]	Windows NT 4.0/2000, Unix	nCipher Support Software 6.00	A vulnerability exists in the 'generatekey' command line utility when either the command line utility 'generatekey' or the 'KeySafe' graphical application is used to import a software based key due to insecure management and removal of files, which could let a malicious user obtain access to key information.	Workaround available at: http://www.ncipher.com/support/advisories/advisory7_keyduplicates.html	nCipher Support Software Key Import Temporary File Cleanup	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Nethack[115] ***Patch & upgrade available***[116]	**Unix**	**Nethack 3.4 .0**	**A buffer overflow vulnerability exists when a specially crafted command string is submitted to the Nethack binary, which could let a malicious user execute arbitrary code.**	***Patch available at:*** **http://nethack.sourceforge.net/v340/bugmore/secpatch.txt** ***Upgrade available at:*** **http://nethack.sourceforge.net/v341/downloads.html**	**Nethack Local Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
NetIQ Corporation Web Trends[117]	Windows NT 4.0/2000, XP, Unix	WebTrends Analysis Suite 7.0	A vulnerability exists due to insufficient sanitization of HTML when logging requests, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WebTrends Logfile HTML Injection	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Netpbm[118]	Unix	Netpbm 10.0-10.14	Multiple buffer overflow vulnerabilities exist due to math overflow errors, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Multiple Netpbm Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[113] Bugtraq, February 24, 2003.
[114] nCipher Security Advisory No. 7, February 25, 2003.
[115] Bugtraq, February 8, 2003.
[116] Bugtraq, March 1, 2003.
[117] Bugtraq, March 4, 2003.
[118] Bugtraq, February 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Netscape [119]	Windows 95/98/ME/ NT 4.0/2000, Unix	Communicator 4.0, 4.04-4.08, 4.5-4.79	A vulnerability exists in the roaming profile function because user credentials are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Netscape Communicator Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Netscape [120]	Multiple	Navigator 7.0	A Denial of Service vulnerability exists in Netscape based browsers when a malicious page that contains a specially crafted JavaScript regular expression method is viewed.	No workaround or patch available at time of publishing.	Netscape JavaScript Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Nokia[121]	Multiple	6210 Handset 5.27	A Denial of Service vulnerability exists when a malicious user submits a malformed vCard that contains format strings.	The vendor has stated that they currently do not plan on releasing a patch for this issue.	Nokia 6210 vCard Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Novell[122]	Windows NT 4.0/2000	Groupwise 6.0, 6.0 SP1& SP2	An unspecified vulnerability has been made public by Novell because WebAccess may be affected by malicious scripts under some conditions. This could result in a violation of local security policy.	Information regarding a fix available at: http://support.novell.com/servlet/tidfinder/2964956	GroupWise WebAccess Malicious Script	Medium	Bug discussed in newsgroups and websites.
Novell[123]	Multiple	iMonitor 2.0	A buffer overflow vulnerability exists which could let a malicious user obtain elevated privileges and possible execute arbitrary code.	Patch available at: http://support.novell.com/servlet/filedownload/ftf/edir870fp1.exe/	Novell NDS iMonitor Unspecified Buffer Overflow	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Novell[124]	Multiple	eDirectory 8.7	A buffer overflow vulnerability exists in DHost, which could let a malicious user obtain elevated privileges and execute arbitrary code.	Patch available at: http://support.novell.com/servlet/tidfinder/2964477	eDirectory Server DHost Buffer Overflow	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[119] Bugtraq, February 28, 2003.
[120] Bugtraq, February 25, 2003.
[121] @stake, Inc. Security Advisory, February 25, 2003.
[122] SecurityFocus, February 20, 2003.
[123] SecurityFocus, February 20, 2003.
[124] SecurityFocus, February 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[125]	Multiple	eDirectory 8.7	A vulnerability exists because it is possible to obtain access to files contained in the \dibfiles directory, which could let a malicious user obtain sensitive information.	Patch available at: http://support.novell.com/servlet/tidfinder/2964477	Novell DIBFiles Directory Access Control	Medium	Bug discussed in newsgroups and websites.
Nuked-Klan[126]	Unix	Nuked-Klan 1.3 beta	Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist in the 'Team', 'News', and 'Liens' modules due to a insufficient sanitization of user-supplied HTML and script code in URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; and information disclosure vulnerabilities exists in the 'Team', 'News', and 'Lien' modules due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Nuked-Klan Multiple Cross-Site Scripting & Information Disclosure Vulnerabilities	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
Opera Software[127]	Windows 95/98/ME/ NT 4.0/2000, XP, Unix	Opera Web Browser 6/0, 6.0 win32, 6.0.1, 6.0.1 win32, 6.0.1 Linux, 6.0.2 win32, 6.0.2 Linux, 6.0.3 win32, 6.0.3 Linux, 6.0.4 win32, 6.0.5 win32, 6.10 Linux, 7.0 win32, 7.0 1win32	A Cross-Site Scripting vulnerability exists due to the way the Opera browser generates a temporary page for displaying a redirection, when 'Automatic redirection' is disabled, which could let a malicious user execute arbitrary script code.	Upgrade available at: http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows	Opera Web Browser Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[125] SecurityFocus, February 21, 2003.
[126] Security Corporation Security Advisory, SCSA-006, February 22, 2003.
[127] Secunia Research Advisory, February 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Pastel Software (Pty) Ltd.[128]	Windows 95/98/ME/ NT 4.0	Pastel Accounting 6.0, 6.1, 6.12	A vulnerability exists in the 'ACCUSER.DAT' file due to insufficient storage of sensitive information, which could let a malicious user obtain access to sensitive information.	No workaround or patch available at time of publishing.	Pastel Accounting ACCUSER. DAT Information Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Point Clark Networks[129]	Unix	Clark Connect Linux 1.2	An information disclosure vulnerability exists in the 'clarkconnectd' service, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://download.clarkconnect.org/clarkconnect-1.2/updates/cc-daemon-1.2-2.i386.rpm	ClarkConnect clarkconnectd 'Remote Information Disclosure	M<edium	Bug discussed in newsgroups and websites. There is no exploit code required.
PY-Livredor[130]	Unix	PY-Livredor 1.0	A Cross-Site Scripting vulnerability exists in the 'index.php' page due to insufficient filtering of HTML tags from various fields, which could let a malicious user execute arbitrary HTML code.	No workaround or patch available at time of publishing.	PY-Livredor Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Real Networks[131]	Windows	Helix Universal Server 8.01, Real Server 5.0, 7.0, 7.0.1, 7.0.2, 8.0 Beta, 8.0 1, 8.0	A buffer overflow vulnerability exists due to insufficient bounds checking of URIs by RTSP methods, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.service.real.com/downloads.html	Real Networks Helix Universal Server/Real Server Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Regents of University of Texas System[132]	Unix	moxftp 2.2	A buffer overflow vulnerability exists in the 'Welcome' banner when remote FTP server messages are parsed, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	moxftp 'Welcome' Banner Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
rxvt[133]	Unix	rxvt 2.6.1-2.7.8	A vulnerability exists because a screen dump feature may be abused to corrupt local files that which are writeable by the terminal user, which could let a local/remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	RXVT Screen Dump Escape Sequence Local File Corruption CVE Name: CAN-2003-0022	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[128] blaqhatz advisory #1, March 3, 2002.
[129] SecurityTracker Alert ID, 1006165, February 25, 2003.
[130] Security Corporation Security Advisory, SCSA-008, March 2, 2003.
[131] Real Networks Security Bulletin, March 3, 2003.
[132] Bugtraq, February 23, 2003.
[133] Bugtraq, February 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
rxvt[134]	Unix	rxvt 2.6.1-2.7.8	A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	RXVT Window Title Reporting Escape Sequence Command CVE Name: CAN-2003-0066	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
rxvt[135]	Unix	rxvt 2.6.1-2.7.9	A vulnerability exists in the MenuBar feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	RXVT Menu Bar Escape Sequence Command Execution CVE Name: CAN-2003-0023	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
SB-Software[136]	Windows, Unix	Logan Pro 1.2	A vulnerability exists due to insufficient sanitization of HTTP header information, which cold let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Logan Pro HTTP Header	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
SCO[137]	Unix	Open UNIX 8.0, UnixWare 7.1.1, 7.1.3	A vulnerability exists because X Server will ignore existing system umask and install files with world readable and writeable permissions, which could let a malicious user cause a Denial of Service, obtain elevated privileges or obtain sensitive information.	Patch available at: ftp://ftp.sco.com/pub/updates/UnixWare/CSSA-2003-SCO.4/basex.pkg.Z	SCO X Server World Writeable Permissions	Low/ Medium (Medium if elevated privileges or sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Siemens[138]	Multiple	Siemens C55, M35 , M45, S35i, S55, SL-42	A Denial of Service vulnerability exists when a malicious user submits a maliciously formed SMS message that contains certain characters.	Contact the vendor about the availability of fixes that address this issue.	Siemens M Series SMS Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited using an SMS client.

[134] Bugtraq, February 24, 2003.
[135] Bugtraq, February 24, 2003.
[136] Bugtraq, March 4, 2003.
[137] SCO Security Advisory, CSSA-2003-SCO.4, March 4, 2003.
[138] Bugtraq, March 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
sircd.org[139]	Unix	sircd 0.4 .0	A buffer overflow vulnerability exists when a reverse DNS lookup is performed due to insufficient bounds checking of user-supplied input, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	Upgrade available at: http://www.sircd.org/files/sircd-cvs.tar.gz	Smart IRC Daemon Remote Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.
Snort Project[140, 141, 142]	Unix	Snort 1.8-1.8.7, 1.9	A buffer overflow vulnerability exists in the network IDS due to a flaw in the RPC preprocessor, which could let a remote malicious execute arbitrary instructions with root privileges.	Upgrade available at: http://www.snort.org/dl/snort-1.9.1.tar.gz **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **SmoothWall**: http://www.smoothwall.org/get/download/patches/1.0-20030304-fixes2.html	Snort RPC Preprocessor Fragment Reassembly Buffer Overflow CVE Name: CAN-2003-0033	**High**	Bug discussed in newsgroups and websites.
Squirrel Mail[143] ***Upgrades now available*** [144]	**Unix**	**Squirrel Mail 1.2.9**	**A Cross-Site Scripting vulnerability exists in the 'read_body.php' script due to a failure to properly sanitize user-supplied parameters, which could let a malicious user execute arbitrary HTML and script code.**	**Debian:** **http://security.debian.org/pool/updates/main/s/squirrelmail/** ***RedHat:*** **ftp://updates.redhat.com/**	**SquirrelMail Cross-Site Scripting** **CVE Name: CAN-2002-1341**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Sun Microsystems, Inc.[145]	Unix	Solaris 2.6, 2.6_x86, 7.0. 7.0_x86, 8.0, 8.0_x86	A vulnerability exists because the FTP client insufficiently guards sensitive information, which could let a malicious user obtain sensitive information.	Patches available at: http://sunsolve.sun.com	Solaris FTP Client Information Guard	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
SurfStats International Ltd. SurfStats[146]	Windows	SurfStats Log Analyzer 6.7 .0.3	A vulnerability exists due to insufficient sanitization of HTML when requests are logged, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	SurfStats Log Analyzer Insufficient Sanitization	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[139] Bugtraq, February 23, 2003.
[140] DHS/NIPC Advisory 03-003, March 3, 2003.
[141] Mandrake Linux Security Update Advisory, MDKSA-2003:029, March 6, 2003.
[142] EnGarde Secure Linux Security Advisory, ESA-20030307-007, March 7, 2003.
[143] Bugtraq, December 3, 2002.
[144] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:042-07, March 4, 2003.
[145] Sun(sm) Alert Notification, 51081, February 27, 2003.
[146] Bugtraq, March 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
tefonline. net[147]	Unix	MyGuest book 3.0	Multiple vulnerabilities exist: a vulnerability exists due to insufficient filtering of HTML tags, which could let a malicious user execute arbitrary code; a vulnerability exists because the existence of a cookie token is solely relied upon when determining the authenticity of a user, which could let a malicious user obtain unauthorized access to administrative pages; and a vulnerability exists due to a failure to validate authenticity of a remote user before taking privileged actions, which could let a remote malicious user modify data.	No workaround or patch available at time of publishing.	MyGuestbook Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the weak cookie authentication and authenticity validation vulnerabilities.
Telindus [148]	Multiple	1120 ADSL Router 6.0.x	A vulnerability exists due to a weakness in the encryption algorithm, which could let a remote malicious user decipher sensitive router information.	No workaround or patch available at time of publishing.	Telindus ADSL Router Encryption Scheme	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Tight VNC[149] ***Upgrade issued[150, 151, 152]***	**Multiple**	**TightVNC 1.2 .0, 1.2.1**	**A vulnerability exists because DES challenges are repeated if multiple connections are initiated in rapid sequence, which could let an unauthorized malicious user obtain access.**	***RedHat:*** **ftp://updates.redhat.com/** ***Mandrake:*** ***http://www.mandrakesecure.net/en/ftp.php***	**TightVNC Repeated Challenge**	**Medium**	**Bug discussed in newsgroups and websites.**
Tim Stoehr[153]	Unix	Rogue 985.0	A buffer overflow vulnerability exists in the 'save game' feature due to insufficient bounds checking of user-supplied input, which could let a malicious user obtain elevated privileges and execute arbitrary code.	No workaround or patch available at time of publishing.	Rogue 'Save Game' Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[147] Bugtraq, February 21, 2003.
[148] Bugtraq, February 23, 2003.
[149] Bugtraq, July 24, 2002.
[150] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:041-12, February 20, 2003.
[151] Mandrake Linux Security Update Advisory, MDKSA-2003:022, February 24, 2003.
[152] Gentoo Linux Security Announcement, 200302-16, February 24, 2003.
[153] SecurityTracker Alert, 1006152, February 23, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Typo3[154]	Multiple	Typo3 3.5b5	Multiple vulnerabilities exist: a vulnerability exists in the 'showpic.php' and 'thumbs.php' scripts, which could let a remote malicious user obtain sensitive information; a vulnerability exists in the log files, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary system commands; an information disclosure vulnerability exists in several scripts, which could let a malicious user obtain sensitive information; a vulnerability exists because several directories are installed by default into the webroot, which could let a malicious user obtain sensitive information; and a vulnerability exists because sensitive data that has been concealed through hidden form fields may be accessed by a malicious user.	Patch available at: http://212.242.92.43/t3dl/typo3_src-3.5.0.tgz	Typo3 Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit scripts have been published. Information Disclosure vulnerability can be exploited via a web browser.
U.S. Robotics[155]	Multiple	Broadband-Router 8000A/8000-2 2.5	A Denial of Service vulnerability exists when a malicious user submits an overly long GET request.	No workaround or patch available at time of publishing.	Broadband-Router GET Request Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[154] 2002@WebSec.org Security Report, February 28, 2003.
[155] SecurityFocus, March 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
University of Kansas[156] ***Vendors issue upgrades***[157, 158, 159]	**Multiple**	**Lynx 2.8.2 rel.1- 2.8.4 rel.1, 2.8.5 dev.8**	**A vulnerability exists when carriage return and line feed (CRLF) characters are included in the commandline, which could let a malicious user make scripts that use Lynx for downloading files from the wrong site on a web server with multiple virtual hosts.**	**Patch available at:** **ftp://lynx.isc.org/lynx2.8.4/patches/lynx2.8.4rel.1c.patch** **Debian:** http://security.debian.org/pool/updates/main/l/lynx-ssl/ **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/3.1.1 **Trustix:** http://www.trustix.net/pub/Trustix/updates ***RedHat:*** **ftp://updates.redhat.com/** ***OpenPKG:*** **ftp://ftp.openpkg.org/release/1.1/UPD/lynx-2.8.4-1.1.1.src.rpm** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**Lynx Command Line URL CRLF Injection** **CVE Name: CAN-2002-1405**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**
Veritas Software[160]	Unix	Bare Metal Restore 3.1, 3.1.1, 3.2, 3.2.1	A vulnerability exists in BMR for Tivoli Storage Manager, which could let a remote malicious user execute arbitrary code with the privileges or root.	Patch available at: http://ftp.support.veritas.com/pub/support/products/Bare_Metal_Restore_for_TSM/patch-TSM-3.2.1-004_254666.tar	Bare Metal Restore for Tivoli Storage Manager Remote Root Access	**High**	Bug discussed in newsgroups and websites.
Webdev[161]	Windows, Unix	Webchat 0.77	A vulnerability exists in the 'defines.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Webchat Defines.PHP Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Web-ERP[162]	Unix	Web-ERP 0.1.4	A vulnerability exists because access to the configuration file is insufficiently restricted, which could let a remote malicious user obtain sensitive information and full access to the underlying database.	No workaround or patch available at time of publishing.	Web-ERP Configuration File	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[156] Bugtraq, August 19, 2002.
[157] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:029-06, February 12, 2003.
[158] OpenPKG Security Advisory, OpenPKG-SA-2003.011, February 18, 2003.
[159] Mandrake Linux Security Update Advisory, MDKSA-2003:023, February 24, 2003.
[160] SecurityTracker Alert ID, 1006172, February 26, 2003.
[161] Bugtraq, March 3, 2003.
[162] SecurityTracker Alert ID, 1006189, March 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Xfree86[163]	Unix	XFree86 X11R6 4.0, 4.0.1, 4.0.3, 4.1.0, 4.2.0, 4.2.1	A vulnerability exists in xterm's window title reporting feature, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	XTerm Window Title Reporting Escape Sequence CVE Name: CAN-2003-0063	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Xfree86[164]	Unix	XFree86 X11R6 4.0, 4.0.1, 4.0.3, 4.1.0, 4.2.0, 4.2.1	A Denial of Service vulnerability exists due to a failure to sufficiently filter certain malicious loop-based escape sequences.	No workaround or patch available at time of publishing.	Xterm Loop-Based Escape Sequence Denial of Service CVE Name: CAN-2003-0071	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
XFree86 [165]	Unix	X11R6 4.2.0, 4.2.1	A buffer overflow vulnerability exists due to the way the 'XLOCALEDIR' string is handled, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	XFree86 XLOCALE DIR Local Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.
YaBB SE[166] ***Work-around available*** [167]	**Unix**	**YaBB SE 1.4.1, 1.5 .0**	**A vulnerability exists in the 'Packages.php' file, which could let a remote malicious user execute arbitrary code.**	***Workaround available at:*** **http://www.yabbse.org/community/index.php?board=9;action=display;threadid=17919**	**YABB SE Packages.PHP Remote File Include**	**High**	**Bug discussed in newsgroups and websites. Exploit has been published.**

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[163] Bugtraq, February 24, 2003.
[164] Bugtraq, February 24, 2003
[165] Securiteam, March 7, 2003.
[166] Bugtraq, January 21, 2003.
[167] SecurityFocus, February 26, 2003.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between February 21 and March 4, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 30 scripts, programs, and net-news messages containing holes or exploits were identified. Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
March 4, 2003	85deadelf.c	Script that exploits the File ELF Routine Buffer Overflow vulnerability.
March 4, 2003	Crashzlib.c	Script that exploits the Zlib gzprintf() Buffer Overflow vulnerability.
March 4, 2003	Linux86_sendmail.c	Script that exploits the SendMail Header Processing Buffer Overflow vulnerability.
March 4, 2003	Zlib.c	Script that exploits the Zlib gzprintf() Buffer Overflow vulnerability.
March 3, 2003	Genraid3r.c	CGI exploit generator that enables an engineer to test standard known CGI exploits with a utility that is customizable.
March 3, 2003	**Lhttpd00r.c**	**Script that exploits the Light HTTPD Buffer Overflow vulnerability.**
March 3, 2003	**lhttpdxpl.c**	**Script that exploits the Light HTTPD Buffer Overflow vulnerability.**
March 2, 2003	0x333cya.tar.gz	Exploit for printer-drivers vulnerabilities.
March 2, 2003	**Oc-localx.c**	**Script that exploits the XFree86 XLOCALE DIR Local Buffer Overflow vulnerability.**
March 2, 2003	ST-tcphump.c	Script that exploits the TCPDump Malformed ISAKMP Packet Remote Denial of Service vulnerability.
March 2, 2003	**Xscreensaver.c**	**Script that exploits the XFree86 XLOCALE DIR Local Buffer Overflow vulnerability.**
February 28, 2003	Showpic.pl	Perl script that exploits the Typo3 Multiple Vulnerabilities.
February 28, 2003	Typo3.pl	Perl script that exploits the Typo3 Multiple Vulnerabilities.
February 27, 2003	LOCATOR-Proof-of-concept.zip	Exploit for the Windows Locator Service Buffer Overflow vulnerability.
February 26, 2003	F-prot.pl	Perl script that exploits the F-Prot Antivirus Command Line Scanner Buffer Overflow vulnerability.
February 26, 2003	**Hoagie_amx.c**	**Script that exploits the AMX Mod Remote 'amx_say' Format String vulnerability.**
February 26, 2003	**Hoagie_bf1942_rcon.c**	**Script that exploits the Battlefield 1942 Remote Buffer Overflow vulnerability.**
February 25, 2003	**Cpanel-VH.pl**	**Script that exploits the CPanel 5 ‘gueltbook.cgi’ vulnerability.**
February 25, 2003	**Cutenews_exploit.php**	**Exploit for the CuteNews Remote File Include vulnerability.**
February 25, 2003	**Html.exe.zip**	**Exploit for the Internet Explorer Self Executing HTML File vulnerability.**
February 25, 2003	**Jocz.pl**	**Script that exploits the CPanel 5 ‘gueltbook.cgi’ vulnerability.**
February 25, 2003	Macstumbler-06b.tgz	An application for Mac OS X that scans and detects wireless networks using an Airport card.
February 24, 2003	Mamboexp. Phps	Exploit for the Mambo Site Credential Authentication vulnerability.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
February 23, 2003	Ex_stmkfont.sh	Exploit for the HP-UX 'stmkfont' Buffer Overflow vulnerability.
February 23, 2003	Moxftp.txt	Exploit for the moxftp 'Welcome' Banner Buffer Overflow vulnerability.
February 23, 2003	Sircd.sh	Exploit for the Smart IRC Daemon Remote Buffer Overflow vulnerability.
February 23, 2003	Sircd.txt	Exploit for the Smart IRC Daemon Remote Buffer Overflow vulnerability.
February 22, 2003	**Webmin-exploit.pl**	**Perl script that exploits the Webmin/ Usermin 'Miniserv.pl' Authentication Bypass vulnerability.**
February 21, 2003	Ooopspf.c	Script that exploits the Cisco IOS OSPF Neighbor Buffer Overflow vulnerability.
February 21, 2003	**Perl2exe_poc.pl**	**Perl script that exploits the Perl2Exe Code False Sense of Security vulnerability.**

Trends

- **The Department of Homeland Security (DHS), National Infrastructure Protection Center (NIPC) has issued an advisory to heighten awareness of the recently discovered Remote SendMail Header Processing Vulnerability (CAN-2002-1337). NIPC has been working closely with the industry on vulnerability awareness and information dissemination. For more information, see 'Bugs, Holes & Patches' table and DHS/NIPC Advisory 03-004 located at: http://www.nipc.gov/warnings/advisories/2003/03-004.htm.** ***Note: SendMail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many SendMail servers are not typically shielded by perimeter defense applications.*** **Remote malicious users may gain access to other systems through a compromised SendMail server, depending on local configurations.**
- Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.
- Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.
- NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:
  - http://www.microsoft.com/security/slammer.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-061.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
- The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.
- The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.
- The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Bugbear	Worm	Increase	September 2002
3	W32/Sobig	Worm	Stable	January 2003
4	W32/Avril	Worm	Stable	January 2003
5	W32/Yaha	Worm	Decrease	February 2002
6	JS/NoClose	Trojan	Stable	May 2002
7	Elkern	File Infector	Slight Increase	October 2001
8	Funlove	File	Slight Increase	November 1999
9	W32/Nimda	File, Worm	Slight Increase	September 2001
10	W32/SQLSlammer	Worm	Decrease	January 2003

Note: Virus reporting may be weeks behind the first discovery of infection. A total 203 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 323 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

IRC-Worm.Blackout (IRC Worm): This is an IRC worm that spreads via IRC channels. The worm itself is a Word document and contains one macro called "Blackout." When the worm is executed, it adds the value "Level 1" to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security

It attempts to disable the Security menu item in the Macro menu and creates in the root directory of the C: disk a file called "blackout.vxd" in which it writes the source code. Additionally this file is used to infect all Word documents in the directory C:\mydocu~1.

IRC-Worm.Evion (IRC Worm): This is an IRC worm that spreads via IRC channels. The virus is written in Visual Basic Script (VBS). It overwrites .vbs and .html files on all local and mapped drives. When the worm is executed, it creates copies of itself in the root directory of disk C: in the file "Win32 Strt.exe.vbs " and in the system directory file "BootLoader.exe.vbs" as well as in the root Windows directory in the files"Jokes.htm" and "Winupdate.exe." It overwrites these existing files with copies of itself.

VBS.Krim.D@mm (Aliases: I-Worm.LoveLetter, VBS/Rimko@mm) (Visual Basic Script Worm): This is a variant of the VBS.Krim@mm worm. It sends itself to all the contacts in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: Symantec center
- Attachment: Vale.bat

If VBS.Krim.D@mm finds that mIRC is installed on your computer, the worm modifies the mIRC Script.ini file. This modification causes the worm to spread over the IRC network.

VBS.Krim.E@mm (Visual Basic Script Worm): This is a variant of the VBS.Krim@mm worm. It sends itself to all the contacts in the Microsoft Outlook Address Book. When VBS.Krim.E@mm is run, a file created by the worm (Vbs.vbs) will display a message containing the Web site address, http://www.newmafiamirko.cjb.net. The e-mail has the following characteristics:

- Subject: La tua amica Valentina
- Attachment: mms.bat

If VBS.Krim.E@mm finds that mIRC is installed on your computer, the worm modifies the mIRC Script.ini file. This modification causes the worm to spread over the IRC network. The worm also attempts to format the C drive by adding a command to the Autoexec.bat file.

VBS.Krim.F@mm (Aliases: Bloodhound.VBS.Worm, I-Worm.Zokrim, VBS/Vale@mm.gen) (Visual Basic Script Worm): This is a variant of VBS.Krim@mm. This worm sends itself to all the contacts in the Microsoft Outlook Address Book. When VBS.Krim.F@mm is run, one of the files that the worm created titled, Mhr.vbs, displays a message box. The e-mail may have the subject, "Mi ami ancora ???" or "Sto male senza di TE." The attachment is named amore.bat. If VBS.Krim.F@mm finds that mIRC is installed on your computer, it replaces the mIRC Script.ini file with its own ini file. This modification causes the worm to spread over the IRC network. The worm also attempts to format the C drive, by adding a command to the Autoexec.bat file.

VBS.Lisa.A@mm (Visual Basic Script Worm): This is a mass-mailing worm that is written in the Visual Basic Scripting (VBS) language. This worm attempts to spread through Microsoft Outlook, mIRC, and KaZaA. The e-mail arrives with a subject of "Click YES and vote against war!." There is no mail attachment as the worm is distributed as script in the body of the e-mail. VBS.Lisa.A@mm may create up to 5,000 folders on the C drive and may delete critical system files. On Windows 95/98/ME computers, the worm may format the C drive.

VBS.Lunnet.A (Visual Basic Script Worm): This is a Visual Basic Script worm that attempts to spread using the KaZaA and Grokster file-sharing networks. The worm also attempts a Denial of Service attack on www.ytunnel.digitalcitrus.com. VBS.Lunnet.A adds a command to the Autoexec.bat file to format the hard drive the next time you start the computer.

VBS.MetSex@mm (Visual Basic Script Worm): This is a mass-mailing worm that is written in the Visual Basic Scripting (VBS) language. When VBS.MetSex@mm is executed, it copies itself to several locations on your computer. It infects all the .txt, .doc, .inf, .bak, .htm, and .html files in all the local and network drives and mails itself to all the contacts in all the Microsoft Outlook Address Books. The e-mail has the following characteristics:

- Subject: <contact name>. HAVING TROUBLE WITH YOUR WINDOWS® ?
- Attachment: NTHelp.vbs

VBS.Naughtypic (Visual Basic Script Worm): This is a polymorphic Visual Basic Script (VBS) worm that attempts to copy itself as the following files:

- C:\Program Files\KaZaA Lite\My Shared Folder\Avril.jpg.vbs
- C:\Program Files\KaZaA Lite\My Shared Folder\Norton's 2003 Crack Gen.exe.vbs
- C:\Windows\System32\MScript32.vbs

VBS.Naughtypic also creates the files, C:\Documents and Settings\All Users\Start Menu\Programs\Startup\Naughty.jpg.

YOUGDOS.A (File Infector): This virus infects .EXE files by attaching its virus code at the start of target files. It also has capabilities to send itself via e-mail and Internet Relay Chat (IRC). Upon execution, it drops the following files:

- C:\mail.vbs
- C:\run.reg
- C:\Windows\s.vbs

MAIL.VBS facilitates the sending of this virus to 20 target recipients listed in the Microsoft Outlook address book. It sends e-mail with the following details:

- Subject: Kewl shit!
- Attachment: mirc69.exe

RUN.REG is this malware's registry component. It modifies the registry so that the dropped file, S.VBS, automatically executes during startup. S.VBS creates a shortcut entry in the desktop named "InternetExplorer.lnk." This entry carries the Internet Explorer icon but actually points to the malware file MAIL.VBS. This virus runs on Windows 95, 98, ME, XP, NT, and 2000 systems.

W32.AimVen.Worm (Alias: Worm.Wom32.AimVen) (Win32 Worm): This worm uses America OnLine (AOL) Instant Messenger (AIM) to spread itself, by modifying the AIM program itself. When W32.AimVen.Worm is executed, it copies itself to the C drive as C:\V.exe and locates and modifies the file, C:\Program Files\AIM95\Icbmft.ocm. (This path is hard-coded.) Once the Icbmft.ocm file is modified, each time you send a .exe file using AIM, a copy of W32.AimVen.Worm will overwrite this file.

W32.Bibrog.B@mm (Alias: W32/Bibrog.b@MM) (Visual Basic Script Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. When the worm is executed, it opens a program that looks like a shooting game and may also change your Windows wallpaper. The e-mail message has the following characteristics:

- Subject: Fwd:La Academia Azteca
- Attachment: Academia.exe

This worm also attempts to spread through the KaZaA, Grokster, and Morpheus file-sharing networks, as well as through ICQ.

W32.HLLW.Ajja (Win32 Worm): This is a worm that attempts to spread across the KaZaA, Grokster, and Edonkey2000 file-sharing networks. This worm also attempts to delete program files belonging to several antiviral programs. As part of the execution of W32.HLLW.Ajja, a fake "Install" message will prompt you to "Clik!! in Next to Install." It is written in Microsoft Visual Basic, version 6.

W32.HLLW.Cult@mm (Win32 Worm): This is a mass-mailing worm that has backdoor capabilities. It uses e-mail to replicate but sends only to the following domains: hotmail.com, msn.com, yahoo.com, Roadrunner.com, Earthlink.net, and e-mail.com. The e-mail message has the following characteristics:

- Subject: Hi, I sent you an eCard from BlueMountain.com
- Attachment: BlueMountaineCard.pif

W32.HLLW.Cult@mm also attempts to spread using the KaZaA file-sharing network. It is packed with XTPack.

W32.HLLW.Daboom@mm (Win32 Worm): This is a mass-mailing worm that replicates by e-mail. It sends itself to the addresses it finds in the:

- Windows Address Book
- htm and .html files stored in the Internet Explorer cache

The e-mail message has a subject, message, and attachment; all of which are randomly chosen. The attachment will have a .pif file extension. W32.HLLW.Daboom@mm also contains backdoor Trojan capabilities that permit unauthorized access to an infected computer. W32.HLLW.Daboom@mm is a Visual Basic (p-code) application packed with UPX 1.20.

W32.HLLW.Dormin.A@mm (Win32 Worm): This is a mass-mailing worm that sends itself to all the contacts in the Microsoft Outlook Address Book. The e-mail has the following characteristics:

- Subject: Check this out!
- Attachment: FlashMovie.exe

When W32.HLLW.Dormin.A@mm is run, it displays the fake error message, "MacroMedia Shockwave Flash is not installed!"

W32.HLLW.Lovgate.E@mm (Win32 Worm): This is a variant of W32.HLLW.Lovgate@mm. This mass-mailing worm attempts to e-mail itself to all the e-mail addresses that it finds in files that have file extensions beginning with ".ht" (for example, .htm and .hta). The subject and attachment of the incoming e-mail are chosen from a predetermined list. The worm also has a backdoor Trojan capability. By default, the Trojan component listens on TCP port 10,168.

W32.HLLW.Oror.AG@mm (Aliases: I-Worm.Roron.51, Win32/Roron.Z@mm, W32/Oror.gen.c@MM) (Win32 Worm): This is a mass-mailing worm and a variant of W32.HLLW.Oror@mm. This worm attempts to spread using e-mail, mIRC, KaZaA, network shares, and mapped drives. The e-mail attachment will arrive with a .exe or .scr file extensions. W32.HLLW.Oror.AG@mm also attempts to terminate and remove various security products from the infected computer. This threat is written in the C++ language and is compressed with UPX.

W97M.X3 (Alias: W97M.X3.a) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and the Normal.dot template. The virus also inserts and executes a destructive Trojan on your computer. W97M.X3 attempts to overwrite the io.sys file, so that an infected computer will not be able to switch on after restart.

WM97/Van-A (Word 97 Macro Virus): This virus infects active documents when an infected document is closed.

WORM_AGOBOT.D (Aliases: W32/Gaobot.gen) (Internet Worm): This memory-resident worm, related to WORM_AGOBOT.C, which propagates via the KaZaA, Grokster, or Bearshare file sharing networks and via network shared drives. It regularly connects to an Internet Relay Chat (IRC) server as a bot, allowing its remote user to launch a Distributed Denial of Service (DDoS) attack from infected machines. This worm, which affects systems running Windows NT, 2000, and XP, also has backdoor server capabilities and can allow remote users to access and manipulate infected systems. It sends out a notification to its remote user that can contain sensitive information, including application serials and IP addresses.

WORM_CYDOG.A (Aliases: I-Worm.Cydog.A, Win32/Cydog.A@MM, W32/Chowl@MM) (Internet Worm): This worm mass-mails copies of itself using Microsoft Outlook to all e-mail addresses found in the infected system's Outlook address book. It randomly selects its e-mail messages. This worm also propagates copies of itself via KaZaA and other popular peer-to-peer file sharing networks. It drops copies of itself into the following shared folders of the peer-to-peer file sharing programs:

- KaZaA - KaZaa\My shared Folder
- Bearshare - Bearshare\Shared
- Grokster - Grokster\My Grokster
- Morpheus - Morpheus\My Shared Folder
- EDonkey2000 - eDonkey2000\Incoming

It drops a batch file detected as BAT_CYDOG.B and designed to delete certain files. However, the dropped batch file contains errors and does not execute its destructive routine. This UPX-compressed, memory resident worm runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_CYDOG.B (Aliases: W32/Chowl@MM, W32.HLLW.Cydog@mm, I-Worm.Cydog.b, Win32/Cydog.B@mm) (Internet Worm): This memory-resident worm was designed to propagate copies of itself via e-mail, KaZaA, and other popular peer-to-peer file sharing networks. It drops copies of itself in the shared folders of different file sharing applications. This worm displays a fake error message. This worm fails to execute its mailing routine and is not able to send out copies of itself via e-mail. It runs on Windows 95, 98, ME, NT, 2000 and XP.

WORM_FRETHEM.M (Aliases: W32/Frethem.m@MM, I-Worm.Frethem.n, W32/Frethem-Fam) (Internet Worm): This non-destructive, memory-resident variant of WORM_FRETHEM.D propagates via e-mail. It arrives as an attachment with the following details:

- Subject: Re: Your password!
- Attachment: DECRYPT-PASSWORD.EXE, PASSWORD.TXT

On systems with unpatched Internet Explorer, the file attachments automatically execute when this e-mail message is previewed or opened in Microsoft Outlook and Outlook Express. This UPX-compressed worm works in Windows 98, NT, 2000, ME and XP. In Windows 95, it just displays an empty message box, and then terminates.

WORM_GIBE.B (Aliases: I-Worm.Gibe.b, Win32/Gibe.B@mm, W32/Gibe.B@mm, Win32.Gibe.B worm, W32/Gibe-D, Win32.Gibe.B) (Internet Worm): This worm propagates via e-mail, shared folders using KaZaA, and via Internet Relay Chat applications such as mIRC. When propagating via e-mail, it gets its recipients from e-mail addresses listed in the Windows Address Book and addresses remotely retrieved from certain news servers. This worm arrives in an e-mail as a security patch from Microsoft. It sends e-mail with a random subject, message body, and attachment name. This malware works on Windows 95, 98, ME, NT, 2000, XP platforms.

WORM_LOVGATE.C (Aliases: worm.W32/Lovgate.gen@M, W32/Lovgate.c@M, W32.HLLW.Lovgate.C@mm, I-Worm.Supnot.c, Win32/Lovgate.C@mm, Win32.Lovgate.C, W32/Lovgate-B, W32.HLLW.Lovgate.C@mm**) (Internet Worm):** This virus has been reported in the wild. It effectively uses a relatively new social engineering trick by mimicking an autoreply message where it attaches itself. Recipients are enticed into opening the malware attachment since the mimicked message arrives as a reply to a familiar message. It has both backdoor and worm capabilities. As a worm, it spreads via e-mail and network-shared folders. As a backdoor, it allows remote users to access the system through port 10168. To spread across the network, it drops a copy of itself in network-shared folders and subfolders using various file names. Through e-mail, it sends itself by replying to all new messages received in Microsoft Outlook and Outlook Express with a message. Note that the e-mail attachment has the file name of the copy it attempts to drop in network-shared drives. This worm also gathers target e-mail recipients from .HT* (HTML) files found in the current, Windows and My Documents folders and then sends itself as an attachment to all the target addresses using any of these various e-mail messages. By opening 10168, it allows remote users to access and manipulate the affected system, effectively compromising system security. It sends a notification to either of the following e-mail addresses:

- 54love@fescomail.net
- hacker117@163.com

It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_LOVGATE.D (Aliases: Win32/Lovgate.D@mm, I-Worm.Supnot.d, W32.HLLW.Lovgate.D@mm**) (Internet Worm):** This virus is similar to WORM_LOVGATE.C. It uses a relatively new social engineering trick by mimicking an autoreply message where it attaches itself. Recipients are enticed into opening the malware attachment since the mimicked message arrives as a reply to a message familiar to the user. It has both backdoor and worm capabilities. As a worm, it spreads via e-mail and network-shared folders. As a backdoor, it allows remote users to access the system through port 10168. To spread across the network, it drops a copy of itself in network-shared folders and subfolders using various file names. This worm parses all the subdirectories of the current folder where the original worm was executed. From there, it drops a copy of itself in each existing subdirectory until the bottom directory is reached. Through e-mail, it sends itself by replying to all new messages received in Microsoft Outlook and Outlook Express with a message. Note that the e-mail attachment has the file name of the copy it attempts to drop in network-shared drives. This worm also gathers target e-mail recipients from .HT*

(HTML) files found in the current, Windows and My Documents folders and then sends itself as an attachment to all the target addresses using any of a number of e-mail messages. By opening 10168, it allows remote users to access and manipulate the affected system, effectively compromising system security. It runs on Windows 95, 98, ME, NT, 2000, and XP.

WORM_YAHA.P (Aliases: I-Worm.Lentin.m, W32/Yaha.p@MM, W32.Yaha.P@mm, Win32.Yaha.P, W32/Yaha-P)(Internet Worm): The worm uses its own Simple Mail Transfer Protocol (SMTP) engine to send copies of itself via e-mail to addresses found in the following:

- Windows Address Book
- ListCache of .NET messenger
- ListCache of MSN messenger
- Yahoo profiles
- ICQ profiles
- *HoTMaiL*.*ht* (all files with file names containing the string “HoTMaiL" and extensions containing "ht")
- *.*ht* (all files with file names containing the extension "ht")

This worm also spreads via shared network drives, launches denial of service attacks against certain Web sites, and terminates antiviral processes. If the current day is Wednesday, this worm attempts to drop a copy of itself into network-shared drives. It also sets the Internet Explorer home page to “http://www.india&ltblocked&gtnakes.cjb.net.” It runs on Windows 95, 98, ME, NT, 2000, and XP.

Worm.P2P.Tanked (Internet Virus): This is a virus that spreads via the KaZaA file-sharing network. The worm has a powerful backdoor routine that connects to an IRC channel and listens to commands from its "master." The worm itself is a Windows PE EXE file about 100KB in length and written in Microsoft Visual C++. It is compressed by the UPX file compression utility and then encrypted with the "Krypton" Win EXE file encryptor. When the infected file is run, the installation routine gains control. While installing the worm copies itself to the Windows system directory under different names (see below) and registers the file in two system registry auto-run keys. Worm-copy names are:

- "Tanked.11:" "system32.exe"
- "Tanked.13:" "winsys.exe"
- "Tanked.14:" "cmd32.exe"

X97M.Rawo (Aliases: X97M/Rawo, X97M_RAWO.A) (Excel 97 Macro Virus): This is a macro virus that infects Microsoft Excel spreadsheets when they are closed.

X97M.Romlax (Excel 97 Macro Virus): This is a macro virus that infects Microsoft Excel spreadsheets when the virus is run. This macro virus creates the viral module Rom.xla and installs it in "Add-ins."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Backdoor.Acidoor	**N/A**	**Current Issue**
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	**C**	**Current Issue**
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	**N/A**	**Current Issue**
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Yoink	**N/A**	**Current Issue**
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.Plux	**N/A**	**Current Issue**
Backdoor.PSpider.310	**310**	**Current Issue**
Backdoor.Redkod	**N/A**	**Current Issue**
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.SubSari.15	**15**	**Current Issue**
Backdoor.SubSeven.2.15	**2.15**	**Current Issue**
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Unifida	**N/A**	**Current Issue**
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdown	**N/A**	**Current Issue**
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	**N/A**	**Current Issue**
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	**N/A**	**Current Issue**
BackDoor-AQT	**N/A**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Evolut	N/A	CyberNotes-2003-03
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	**N/A**	**Current Issue**
Exploit-IISInjector	N/A	CyberNotes-2003-03
ICQPager-J	**N/A**	**Current Issue**
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	**N/A**	**Current Issue**
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	C	CyberNotes-2003-04
JS_WEBLOG.A	**A**	**Current Issue**
KeyLog-Kerlib	**N/A**	**Current Issue**
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	**N/A**	**Current Issue**
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04

Trojan	Version	CyberNotes Issue #
ProcKill-AE	**N/A**	**Current Issue**
ProcKill-AF	**N/A**	**Current Issue**
ProcKill-Z	N/A	CyberNotes-2003-03
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
QDel359	N/A	CyberNotes-2003-01
Renamer.c	N/A	CyberNotes-2003-03
Tellafriend.Trojan	N/A	CyberNotes-2003-04
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	**A**	**Current Issue**
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	**A**	**Current Issue**
Trojan.Barjac	**N/A**	**Current Issue**
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	**N/A**	**Current Issue**
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	**N/A**	**Current Issue**
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	**N/A**	**Current Issue**
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

Backdoor-AFC (Aliases: Backdoor.Sparta, Backdoor.Spartadoor): When the Server component of this Remote Access Trojan is executed on the victim machine, it will attempt to disable or delete the processes/files of several Antiviral and firewall products. The Trojan copies itself as MDME.EXE to the following folders:

- %System%\SPFILE\
- %Windir%\Start Menu\Programs\StartUp\

It also copies itself as WINFILE.DTA to the %Windir% folder and creates the file:

- %WINDIR%\WINSTART.BAT.

The WINSTART.BAT file includes the following entries:

- "@if exist "C:\WINDOWS\mdme.exe" goto f"
- "@copy "C:\WINDOWS\winfile.dta" "C:\WINDOWS\StartMenu\Programs\Startup\mdme.exe

The following registry key is modified so that the Trojan is executed at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Shell Folders

with the value : "C:\WINDOWS\SYSTEM\spfile." The Trojan then opens port 5969 and connects to a server at "cdeath.zoomph.net." A notification is sent to the malicious user with the victim's machine information such as IP Address, Username and Password. Once the machine has been compromised it allows the malicious user to perform the following actions from a remote location.

BackDoor-AQL: This threat consists of two components: the client and server. Once the server is running on the victim machine, the malicious user is able to connect (and administer that machine) using the client component. When run on the victim machine, the server component opens a TCP socket accepting commands sent from the client on port 2003. This specific variant does not copy itself to any system folder nor does it add a hook to the Registry. The client component offers many functions to the malicious user.

BackDoor-AQT (Aliases: BackDoor.Silver.10, Backdoor.SilverFTP.10, Win32.AnaFTP.01): This is a backdoor Trojan that allows remote access. When run, the Trojan copies itself to C:\windows\system\svchost32.exe. It creates the following registry key in order to run at Windows start up:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Windows Config Loader" = "c:\windows\system\svchost32.exe"

The Trojan opens port 9003 and listens on the port. It contacts a specific web site and sends an ICQ message. The Trojan can perform various backdoor activities such as copying files, running executables, etc.

Backdoor.Acidoor (Alias: Backdoor.Acidoor.11): This is a Backdoor Trojan that gives a malicious user unauthorized access to your computer. By default, it uses ports 4432 and 4433. The existence of the file Extapp.exe is the sign of a possible infection. Backdoor.Acidoor is a Visual Basic application.

Backdoor.Beasty.C (Aliases: Trojan Beast 1.92, Backdoor.Beastdoor.192): This is a backdoor Trojan that is similar to Backdoor.Beasty and Backdoor.Beasty.B. It gives a malicious user complete access to your computer. By default, the Trojan listens on port 666 and notifies the malicious user through e-mail or ICQ. The Trojan attempts to terminate the various security products and system monitoring tools. The Backdoor.Beasty.C Trojan was created using the Delphi programming language and it is an updated version of Backdoor.Beasty.B.

Backdoor.Darmenu: This is a backdoor Trojan that accesses a page on the Web site, www.tonightsmenu.com/ra3soft, and may download instructions from it. It can perform many actions without your permission, such as shutting down the computer, sending a list of files and folders to the malicious user, and so on.

Backdoor.IRC.Yoink (Alias: IRC-Yoink): This is a backdoor Trojan that allows a malicious user to use IRC to remotely control your computer. The existence of the file Sysclean.exe is a sign of possible infection. It can be delivered by various means, including but not limited to e-mail and IRC file transfer. If Backdoor.IRC.Yoink is executed, it connects to the IRC server, marley.mine.nu, on port 6,667 and joins the IRC channel, #des-clan, and announces its presence. Backdoor.IRC.Yoink allows a malicious user to perform the following actions:

- Open an FTP server on your computer and upload and download files.
- Launch a UDP/SYN flood against a designated IP port address.
- Launch an e-mail flood attack against a specified e-mail address

Among the strings found inside of Backdoor.IRC.Yoink is the string: steve_waugh.

Backdoor.Plux: This Trojan opens a listening port on your computer. This action could allow a malicious user to remotely control your computer. Backdoor.Plux uses web.icq.com to send a message to the malicious user's ICQ Unified Messaging Center. This message includes the IP address of the infected computer.

Backdoor.PSpider.310 (Aliases: Backdoor.PowerSpider.310, BackDoor-AQO): This Trojan allows unauthorized access to your computer. It is a key-logger that records all the keystroke and Input/Output (I/O) streams.

Backdoor.Redkod: This is a backdoor Trojan that gives a malicious user full control over your Windows NT/2000/XP computer. By default the backdoor listens on port 58666.

Backdoor.SubSari.15: This is a Trojan that allows unauthorized access to and control of your computer. It also steals passwords. When Backdoor.SubSari.15 is run, it copies itself as C:\Command.exe and adds a line to the Autoexec.bat to execute Command.exe when you start Windows. Next, it creates the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Burdamýsýn

and chooses a port for the Trojan to use. The default ports begin with 1090 and increment each time the Trojan is run. Other variants of this Trojan use ports 39, 3131, and 6711. There may be a configuration program that allows the client to set the access ports. This Trojan is written in Delphi and ostensibly originated in Turkey.

Backdoor.SubSeven.2.15: This is a variant of the Backdoor.SubSeven Trojan horse. Backdoor.SubSeven.2.15 allows a malicious user to access and control your computer. When it run, it creates the registry key:

- HKEY_LOCAL_MACHINE\Software\SubSeven

in which it stores all of the Trojan's client information. The malicious user can configure the port configuration on the server, as well as the startup methods (registry key values). This version of the Trojan contains:

- Keylogger functions
- Chat functions that allow the malicious user to use Internet Relay Chat (IRC) to control your computer
- An IP scanner that searches for random IP addresses to infect Instant Messenger and ICQ spy functionality
- Functionality that allows the malicious user to directly modify the registry, change the "look and feel" of your computer, and enable a Webcam if one is installed.

Backdoor.Unifida (Alias: Backdoor.Unifida.13): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. This Trojan may release password information obtained from the system's password cache to the malicious user. It is a Visual Basic application that is packed using PECompact, v1.50.

Backdoor.Zdown (Aliases: TrojanDownloader.Win32.Zdown.11, Downloader-BU): This is a backdoor Trojan that gives a malicious user unauthorized access to your computer. This backdoor also attempts to disable various antiviral and firewall programs by terminating active processes. Because a Trojan generator produced Backdoor.Zdown, its features are preprogrammed.

Downloader-BW (Aliases: Small.n, Webmoney Trojan): When this Trojan is run, it shows a fake error message. The downloader attempts to download 2 files from the www.yahoo-greeting-cards.com website. The two files are:

- DBOLE.EXE
- SICKBOY.EXE

These files are dropped in to the %System% directory. The SICKBOY.EXE file is renamed to SYSVIEW.EXE file. The following registry key is updated so that the files run after every restart:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

with the values:

- "DatabaseOLE" = "%winsysdir%\dbole.exe"
- "SystemView" = "%winsysdir%\sysview.exe"

IRC/Flood.ap (Aliases: Q8Hell, Worm.Win32.Randon): This is a Virus-Worm distributed via IRC-channels and LANs with shared resources. When executed, this worm installs its components into the subdirectory zxz and/or zx in the Windows system directory and registers its main file and the mIRC client in the Windows registry auto-run key:

- HKLM\\Software\Microsoft\Windows\CurrentVersion\Run\updateWins

Randon then executes the above key and hides the process via the HideWindows utility. It connects to the IRC-server and executes its scripts. In addition to DDoS attacks and IRC channel flooding, Randon scans port 445 of other IRC clients. Upon detection of an open port (445) the worm runs the batch files sencs.bat and incs.bat which try to locate open resources on the remote computer and connect to them using one of the following passwords: "admin," "administrator," "root," "admin," "test," "test123," "temp," "temp123," "pass," "passwor," and "changeme." If a connection is successful the worm opens a socket on port 445, transfers the Trojan horse TrojanDownloader.WIn32.APher.gen and runs it. This Trojan downloads a self-extracting archive of the worm's 'full' version from "www.q8kiss.net" and installs it in the system.

ICQPager-J: This Trojan is designed to send notification messages to the malicious user from the victim machine. It comprises various components: server, server editor (for configuration) and scripts (ASP, CGI, PHP). When the server component is run on the victim machine, it copies itself to that machine (path and location are configurable in the server, default is C:\TEST.EXE) and adds a startup hook into WIN.INI. An outgoing DNS request is then sent for a remote ICQ server. If satisfied, the notification is then sent to the malicious user via HTTP using a script on that server. The details contained within the notification are configurable via the configuration component. The configuration component enables the malicious user to edit the notification server and create servers that notify via SMS, ICQ or ASP/CGI/PHP. Configurable parameters include:

- recipient address (ICQ or cell number)
- message contents
- installation path/filename
- URL for ASP/CGI/PHP script

JS_WEBLOG.A: This JavaScript Trojan retrieves all data entered in HTML Web forms on Internet Explorer. It then sends the retrieved data to a particular Web site or to a particular system on the same network. It affects systems running Internet Explorer on Windows 95, 98, ME, NT, 2000, and XP.

KeyLog-Kerlib: This is a simple key logging Trojan, designed for Windows NT. When run, the Trojan simply captures the Windows title, and typed keystrokes as they are entered in to the top most Window. Entries are logged to the file C:\WINNT\KERNEL32.DLL.

Linux/Exploit-SendMail: This malware uses vulnerability in SendMail. By sending a malformed message to a victim it gains access of the system where it can execute arbitrary code with the permissions of the running SendMail daemon. The vulnerability occurs when SendMail tries to verify the syntax of the addresses in the envelope (From:, To:, CC:, etc). A specially crafted address can be used to exploit a buffer overflow in the checking code. Because the exploit is fully contained in the message it is possible for a not vulnerable mail transport agent to forward the infected message to other systems. This makes it theoretically possible for the malicious user to rely on a not vulnerable mail border gateway to access vulnerable systems in an Intranet.

ProcKill-AE: This Trojan attempts to terminate the process of various security programs. This Trojan does not add itself to any autostart keys or copy itself to the Windows directory, so simply rebooting the computer will clear the Trojan from memory. However, a dropper or installer component could install it to run at Windows startup.

ProcKill-AF: This Trojan attempts to terminate the process of various security programs. It also searches for processes with a list of strings taken from the above list, minus the ".exe" extension. Any processes which it finds which match, it will also terminate. This Trojan does not add itself to any autostart keys or copy itself to the Windows directory, so simply rebooting the computer will clear the Trojan from memory. However, a dropper or installer component could install it to run at Windows startup.

TROJ_RACKUM.A (Alias: W32/Rackum.worm): This is a floppy worm and key logging Trojan. When run, the worm displays a fake error message. The worm copies itself to the WINDOWS SYSTEM (%SysDir%) directory as Wind32reg.dll.exe and creates a registry run key to load itself at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Win32reg.dll" = C:\WINDOWS\SYSTEM\Wind32reg.dll.exe

Every five minutes the worm copies itself to the A: drive as Letter.txt.exe. The system time, typed keystrokes, and Window titles are stored in a buffer as system events occur. Every 20 seconds the contents of the buffer are appended to the file %SysDir%\Winsck32.sys.Txt. Every six hours this file is e-mailed via SMTP to the author, with the following information.

- From: Bond@007.com
- To: ciakukarm@yahoo.com
- Subject: This is a message for you!
- Attachment: Winsck32.sys.Txt

The worm contains a payload to delete the following files:

- regedit.exe
- msconfig.exe

Troj/Slacker-A (Alias: W32.Slackor, Worm.Win32.Slackor): This is a complex Trojan that may be installed by Troj/Yabinder or any other generic Trojan dropper. It may be delivered separately or packed within cnn3.exe that is a variant of Troj/Yabinder. When executed, cnn3.exe creates a new folder in the root folder with the name SP and extracts the following files to the new folder, setting their attributes to hidden:

- abc.bat
- main.exe
- psexec.exe
- slacke-worm.exe

Cnn3.exe then spawns slacke-worm.exe. Slacke-worm.exe runs in the background as a "netbios auto-router by eRiC" VB application and searches for available IP addresses with no password or a weak password (on port 445). Slacke-worm.exe then calls abc.bat, with the relevant computer name, which tries a list of passwords for the administrative accounts and then uses psexec.exe to copy over and run main.exe on the remote computer.

Trojan.Barjac: This Trojan e-mails the system information to the Trojan's author. This information includes the computer name, IP address, Microsoft Outlook e-mail addresses, and files that have the .doc extension. It sends the e-mail to a tiscali.ch e-mail address, using the SMTP server 212.40.5.65 (mail.tiscalinet.ch)

Trojan.Grepage (Aliases: Trojan.Win32.Grepage, Grepage, TROJ_GREATPAGE.A): This is a Trojan horse that opens a particular Web site in the default browser every 30 seconds. When the Web site is opened, the Trojan "freezes" the cursor. It does not have a malicious payload and only performs this unwanted action.

Trojan.Poot: This is a Windows device driver that intercepts the file, folder, registry, and process calls. The device driver can hide certain files, folders, registry entries, and processes from you. Another program must install Trojan.Poot, which has been found on systems as the file, P2.system

VBS.Trojan.Lovcx (Alias: Trojan.VBS.Lovcx): This is a Visual Basic Script (VBS) Trojan that is similar to the VBS.Loveletter.CV@mm worm. It copies itself to the \Windows\System folder as Msword.vbs and Thwin.vbs, deletes up to five files that have certain file extensions, saves a list of the deleted files as \Windows\System\ListWin.txt, and may also attempt to copy itself to the A drive. Unlike VBS.Loveletter.CV